1. What are your views on the idea of linking social media accounts to Aadhar? Will it be beneficial in any way from the perspective of India's internal security? Critically Comment.

Introduction

Recently, Tamil Nadu government told the Supreme Court that social media profiles should be linked to users Aadhaar number to check terrorist messages, pornography, and fake news.

Body

Good Idea, can be looked after

- With the increase in number of fake news posts on social media, this can help with identifying the originator of fake news, with intentions are to create tensions in the society.
- Recent issue of online Blue Whale game, which led to suicides of many. It was difficult for the government to trace the originator.
- It is estimated that around 15% of twitter accounts are by bots, these bots are not human run, still they play a big role in spreading fake news.
- The increase in crimes such as Child pornography, Revenge porn, morphed photographs etc are on rise.
- Many anti-national posts and hate posts too are on rise, this creates social unrest.
- Social Media companies too have failed to keep a check on such posts despite receiving complaints.

Concerns

- There are many privacy concerns, this might be in conflict with the recent Aadhaar Judgement.
- Whatsapp has recently said that it cannot share the Aadhaar number with a third party as the content on its instant messaging Whatsapp was end-to-end encrypted and even they do not have access to it.
- Large number of fake news is generated from foreign nations too, this provision won't be able to address the issue.
- There is concern with regards to fair investigation, government might burst heavily on its critics too.
- Facebook reported the issue of Cambridge Analytica two years from the incident, with the absence of data localisation, how safe would Aadhaar details be stored with social media companies.

Yes, It can address India's internal security issues

- Social Media has the potential to mobilize large crowds, there exists threat to peace when crowd attempts to disturb the atmosphere. Hence, precautionary steps can be taken, if authorities are aware of such events.
- The offensive clips and hate messages have created social unrest like observed in Muzzaffarnagar riots 2013, Assam Ethnic clashes 2012 etc, spread of such videos and posts can be curtailed.
- Social media has become a potent tool for radicalisation by terror groups, arrest of Mehdi Masoor Biswas, in 2014, accused of being the man behind terror group Islamic State's (ISIS) most influential Twitter handle in India, brought to surface the extent of the threat posed by the misuse of social media.
- There is always a virtual community in social media that attempts to bring in political instability and revolution, sometimes using anti-national posts.
- The recent phenomena of Urban Naxals, who use the social media platform to reach out to naxalites.

However, there might exist few challenges. Most of the cyber terrorism originates from outside the national boundaries. Open-Source monitoring is possible, but monitoring of personal conversations will spark off debate.

Way Forward

- Social media companies need to be made compliant with Indian laws, when operating in India.
- Social media companies should be forced to ensure that they should store the metadata of all the content that is uploaded and by whom, they should store the details of the source.
- Laws can be made as per the recommendations of BN Srikrishna report on "Data Protection".
- Social Media lab (2013) Model of Maharashtra can be worked upon.

Conclusion

As stated by Supreme Court, there is a need to find a balance between the right to online privacy and the right of the state to trace the origins of hateful messages and fake news. Any state intervention for regulation of online content has to pass the test of proportionality laid down by the Supreme Court in Puttaswamy Privacy judgement.

2. Social media platforms have become a major source of fake news and propaganda. Do you agree? How does it threaten peace and order in the country? How can it be addressed? Analyse.

Introduction:

Fake news, or hoax news, refers to false information or propaganda published under the guise of being authentic news. Fake news websites and channels push their fake news content in an attempt to mislead consumers of the content and spread misinformation via social networks and word-of-mouth.

Body:

Fake news is made-up stuff, masterfully manipulated to look like credible journalistic reports that are easily spread online to large audiences willing to believe the fictions and spread the word. This has, in turn, led to deliberate propaganda and clickbait articles causing disharmony in the country.

Fake News poses a security threat to peace and order in the country:

- **Social rifts**- Burial of real news, and spread of fake news create rifts among communities and castes and also polarize people along ideological lines. Ex. cow vigilantism
- **Mob violence**- Fake news of a certain person being a 'child-lifter' led to the death of an innocent civilian by the mob.
- **Hate speech**- Hate speeches are spread through communal media to incite violence.
- **Riots**- With fake information, it can lead to riots between two religious groups or community groups Ex. Muzaffarpur riots.
- **The radicalisation of youth:** The modus operandi of ISIS was the usage of social media to spread the fake and false messages and target vulnerable youth and radicalize them. Ex. The radicalisation of youth in the state of Kerala.
- **Impacted morale of soldiers**- Fake news like soldiers will have to spend their own money to buy uniforms and other clothes from civilian markets hurt the morale of the forces and the families of forces.
- **Damage to reputation**- Spreading fake news about a person, or using a picture of someone in fake news can damage the person's reputation and even lead to harassment and intimidation. Ex. JNU doctored video.

How to address fake news problem:

- **Accountability of social media**- Like WhatsApp limiting forwards, other social media platforms should also have accountability to deal with such news. Social Media platforms have to filter the spread of fake news.
- **Education campaign**- This education campaign needs to carried out by the apps and platforms, as well as the government about the education of the do's and don'ts, and the laws governing the conduct of participants.

- **Screening**- Special screening to check the use of automated software and chatbots responsible for the spread of fake news.
- **Independent agency**- Government appointed an agency to verify data being circulated on social platforms. Officers at the district level to be appointed to gather intelligence and closely monitor social media contents.
- **Private Initiatives**- like AltNews.in, Lallantop, media vigil and Debunked should be taken for a fact check of news and to pull down and debunk fake news.
- **Enforcement**- Platforms and Intermediaries need to comply with data access demands made under India laws by our security agencies.
- **Self-regulation and awareness**- Active civil society to curb the spread of fake news. People themselves must cross-check any news before reacting over it.
- **Punishment**- Severe punishment to be awarded for creating and spreading fake news.
- **Active participation of police**- Local police can be a part of the social media group to constantly check and monitor the spread of news.

Conclusion:

Traditional media had the ways to screen material and verify sources before putting information in the public domain. But in the current world, with the prevalence of social media, we need the participation of all stakeholders to ensure only the information which is true and is beneficial for the society as a whole should see the light of the day.

3. How are external state and non-state actors using various social media platforms to further their agenda in India? Explain. How can such threats be averted? Discuss.

Introduction:

While the advantages of social media are so many, the threats to internal security in various forms like Cyber Terrorism, Fraud, crime, spreading violence, etc. are alarmingly become frequent now. Various external state and non-state actors are using various social media platforms to spread propaganda globally, including in India.

Body:

As internet has increased its reach and has become very accessible, it is a tool effectively used by state and non-state actors to spread 'Internet-enabled' terrorism, spread hate and tensions and disrupt the overall stability through their agenda:

- Radicalisation of youth: Propaganda information to recruit for terror groups like AQIS, LeT on telegram have been intercepted by NIA.

- Use of Internet by Daesh: Daesh has been using Internet to spread its propaganda using platforms such as twitter, YouTube etc.
- Constant involvement and interaction: By 'cyber-planners', who will be responsible for planning terror attacks, identifying recruits, act as "virtual coachers", and provide guidance and encouragement throughout the process.
- In Recruitment from other countries: India is also suffered from it however less severely. Increasing number of cases of youth being influenced by social media to carry out propaganda of hate and violence has been reported in many areas.
- Rise of sentiments over sensitive issues: By spreading false propaganda and fraudulent ideologies over sensitive and triggering issues of India using morphed videos, or false claims of proof of injustice etc.

Precautions to avoid such threats:

- Review of the IT Act to make it stronger and setting up a crack team to respond to unusual incidents on a war footing.
- Strengthening the existing infrastructure : e-Surveillance Projects: National Intelligence Grid (NATGRID), CERT-In, Central Monitoring System (CMS), Internet Spy System Network and Traffic Analysis System (NETRA) of India, National Critical Information Infrastructure Protection Centre (NCIPC) of India etc.
- Strengthening of social networking sites.
- Responsible social media by citizens themselves can avoid a major risk threat.
- Awareness programmes regarding the safe usage of Internet and social media among the people.
- Training and employing ethical hackers to check vulnerabilities present in the cyberspace and respond quickly when there is a cyber-attack.

Challenges:

- **Vulnerability of users**: Several users get blackmailed, or taken advantage of using their vulnerability and misguided knowledge.
- **Server location and laws of different countries**: Lack of geographical boundaries makes social media regulation an arduous task. Major complicating factors to secure the networks and media are a huge concern.
- **Encrypted message and anonymity:** Use of phones/whatsapp to send and receive messages, concerns the government because the communications sent via such devices and applications are encrypted and cannot be monitored and consequently hinders the country's efforts to fight terrorism and crime.

Conclusion:

India has joined a France led initiative to adopt a declaration to counter terrorism and radicalisation online including social media which is a welcome step in tackling this issue. Enhanced cooperation among the wide range of actors with influence over this issue, including governments, civil society, and online service providers, such as social media companies, to eliminate the spread of negative agenda is the way forward.

4. There is a thin line between freedom of expression and irresponsible civic behaviour. Do you think regulations are required to be introduced to make sure this thin line is abided by the social media users? What are the challenges in regulating the social media? Explain.

Introduction

Social Media has become a vital communications tool through which individuals can exercise their right of freedom of expression and exchange information and ideas.

Body

Freedom of expression:

- **Raising voice:** A growing movement of people around the world has been witnessed who are advocating for change, justice, equality, accountability of the powerful and respect for human rights (e.g. Arab Spring Revolution) wherein the Internet and Social Media has played a key role.
- **Hashtag activism:** The term can also be used to refer to the act of showing support for a cause through a like, share, etc. on any social media platform, such as Facebook or Twitter. Example: metoo, saveearth,

Irresponsible civic behaviour:

- **Defamation:** The most affected people through social media are politicians and celebrities. People got another medium to express their anger and to defame them through tweeting or by other social networking sites.
- **False and unreliable information:** People make fake email accounts of celebrities and spread untrue stories about them.
- **Sexual predators:** For example, the most common scenario when a man of 42 years make an email account using fake name and picture of 16 years old boy, communicate to others and ask them to meet in person.
- **Cyberbullying:** Cyberbullying is the act of bullying by harming or harassing using electronic technology. It adds users to the bullies account and begins to bully in the way of harassing the user through teasing, derogatory remarks, etc.

- **Fraud**: for example, person with the attractive profile picture who just friended you, and suddenly needs money -- is probably some cybercriminal looking for easy cash.
- **Religious indoctrination:** viral videos, influence on youth, radicalization of youths are some of the threats.

Regulations are required:

- **Section 66A of the Information Technology Act:** Punishment for sending offensive messages through communication service. It is punishable with imprisonment for a term which may extend to three years and with fine.
- **Section 69 of the Information Technology (IT) Act, 2000**: It has the power to impose reasonable restrictions on this right and intercept, decrypt or monitor Internet traffic or electronic data whenever there is a threat to national security, national integrity, and security of the state.
- **e-Surveillance Projects:** National Intelligence Grid (NATGRID), Central Monitoring System (CMS), Internet Spy System Network and Traffic Analysis System (NETRA) of India, National Critical Information Infrastructure Protection Centre (NCIPC) of India, National Cyber Coordination Centre (NCCC) of India, Tri Service Cyber Command for Armed Forces of India, Cyber Attacks Crisis Management Plan Of India.
- **State Computer Response teams:** Establishment of the State CERT to operate in conjunction ICERT and coordinate with NCIIPC

Challenges in regulating the social media:

- **Targeted phishing attacks:** Such attacks are carried out to steal money or confidential information, as was the case with the Hydraq attacks in early 2010 that compromised critical information of several multi-national companies.
- **Activities across borders:** difficult to trace and take actions related to international crimes.
- **Criminal Activity and Money laundering:** Organised criminals are now using social media to recruit some public individuals to act as unsuspecting money launderers of their money they got from their dirty works like drug smuggling, people trafficking and fraud.
- **Policy framework:** Acts are not stringent and demarcated to take action against the fraud.

Conclusion

It is important to keep the pace with the rapidly changing society. Even today the society is not prepared to bear the consequences of the misuse of social media which will result in the unacceptable and unfamiliar social behaviour.

5. What is bullying? Why has it become so rampant on the social media? How can it be addressed? Discuss.

Introduction

Bullying is when an individual or a group of people with more power, repeatedly and intentionally cause hurt or harm to another person or group of people who feel helpless to respond. Bullying can continue over time, is often hidden from adults, and will probably continue if no action is taken.

Body

Bullying in social media:

- Against the individual feelings: Posting hurtful, nasty or humiliating rumours or comments about an individual online
- Vested intentions: Publishing an embarrassing or nasty photo or video
- Fake news: Creating a fake or nasty webpage about another individual.
- Vulnerable sections: students, adolescents, transgender are easily prone to bullying. Example: In November 2017, an MBBS student in Kerala jumped to her death from the highest floor of her college building. An examination of her Facebook profile showed her displeasure over the nasty comments made one of her peers. Police suspect that cyber bullying provoked her to take this extreme step
- Provoking and influencing: Issuing online threats provoking an individual to kill themselves or hurt someone else
- In the name of religion: Triggering religious, racial, ethnic or political vitriol online by posting hate comments or content
- Online predatory: Faking an identity online to ask for or post personal or fake information about someone

Measures to avoid cyber bullying:

- Be Wary of Your Child's Online Activities: Teenagers and adolescents are more vulnerable to cyber bullying as they have limited understanding of the good and the bad
- Watch keenly regarding emotions: Display of emotional responses such as sadness, anger or happiness to the activities on their device.
- Legal framework: No special Anti-Cyber Bullying Laws in India yet. Following are some cyber laws though that covers some of the acts classified as cyber bullying in India.
- Private institution: Incognito Forensic Foundation (IFF Lab) is a private forensic laboratory in Bangalore and Chennai that offers consultation and digital forensic services for cyber bullying.
- Restore self-respect: Remember that the ultimate goal is to protect and restore the victim's self-respect. Act thoroughly; fast decisions can only make things worse. Talk to someone about the problem before responding.

Conclusion

Recovering from the trauma of cyber bullying can be time-taking and hard. In such cases, the victim needs support and guidance. It could come from parents, peers, family members or teachers. If required, seek the help of a professional counsellor